Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Charter Communications, Inc.'s	)	
Request for Waiver of Section 76.1204 (a)(1)	)	CSR-8470-Z
of the Commission's Rules	)	MB Docket No. 12-328
	)	
Implementation of Section 304 of the	)	
Telecommunications Act of 1996	)	CSR Docket No. 97-80
	)	PP Docket No. 00-67
Commercial Availability of	)	
Navigation Devices	)	

Reply Comments of
Beyond Broadband Technology, LLC

Beyond Broadband Technology, LLC ("BBT") hereby submits its reply comments with respect to Charter Communications above-referenced request for waiver of Section 76.1204(a)(1) of the Commission's rules.

INTRODUCTION

The Commission has long recognized and honored Congress' admonition that, in implementing Section 629 of the Communications Act, the Commission must "...avoid actions which could have the effect of freezing or chilling the development of new technologies and services.."[1] By remaining mindful of this statutory direction, the Commission has paved the way for the development of "downloadable security" – a technological innovation that can serve as the core of a new form of security not only for MVPD video distribution, but also for a vast array of information and data services, including health records, business and government data including military and Homeland Security applications, and the power grid, among others. The development of downloadable security –

[1] H.R. Rep. No. 104-458, at 181 (1996) (Conf. Rep.), *reprinted in* 1996 U.S.C.C.A.N 124,194.

and the substantial public interest benefits that it offers across many sectors using multiple technologies – can be directly traced to the Commission's willingness to allow experimentation and its refusal to rigidly apply rules mandating static technology such as those at issue here.

In particular, the Commission's fealty to Congress' mandate that it not stand in the way of technological innovation was instrumental in allowing and encouraging BBT to develop its downloadable security solution for use by cable television operators. The technology developed by BBT now exists, is in commercial use, and – contrary to the suggestion of the Consumer Electronics Association ("CEA") in its opposition to Charter's waiver request – comports with the expectations articulated by the Commission.

At their core, the arguments of those opposed to Charter's waiver request do not focus on the facts surrounding the current status of downloadable security; rather, they reflect a fundamental misunderstanding of what is already available in the marketplace. In particular, CEA and Public Knowledge ("PK") both contend that instead of encouraging further innovation in the downloadable security arena, the Commission should begin a new round of rulemakings to replace the failed CableCARD approach to separable security with yet another attempt to standardize and freeze technology. Specifically, CEA urges the Commission to create "a nationally standard interface for the direct attachment of retail devices to MVPD systems."[2] PK's comments go even further, suggesting that such an interface should not be located in the retail device, but rather should be in a "gateway" at a single point in the home.[3]

It is noteworthy that the Commission currently is considering what constitutes an "MVPD" in the digital age,[4] an inquiry that is even more fundamental than the question of what technology, if any, the government could or should mandate once it clarifies that basic issue! Clearly PK and CEA are not

[2] CEA Opposition at 10.

[3] PK Comments at 2.

[4] *Media Bureau Seeks Comment on Interpretation of the Terms "Multichannel Video Programming Distributor" and "Channel" as Raised in Pending Program Access Complaint Proceeding*, Public Notice, MB Docket No. 12- 83, DA 12-209 (Mar. 30, 2012) ("Public Notice").

focused on the issue of the ongoing experimentation and development of downloadable security; they seek more, and they want the Commission to freeze technological developments until they get it. This is not the appropriate proceeding to do that. The Commission should steadfastly adhere to its policy of allowing that experimentation and development to continue, as it has with BBT.

DISCUSSION

I. The Current Status of Downloadable Security.

As CEA acknowledges, the FCC has encouraged the development of "downloadable security" as a potentially better alternative to the CableCARD. The Commission was correct to do so. CEA's arguments to the contrary reflect its longstanding confusion over the difference between "security" and "conditional access" – confusion that BBT has repeatedly sought to clear up in a "White Paper" that has been made a part of the record in various proceedings related to the implementation of Section 629.[5] The BBT White Paper explains and cautions that "security" and "conditional access" are two different things and need to be thought of separately.

BBT has developed a downloadable security solution technology which requires an inexpensive hardware component (a secure microchip) embedded in any communications device which can then take advantage of subsequently enabled "downloadable security." The distinction drawn here is that the BBT technology (the "BBT*Solution"*®) establishes a ***secure communications path.*** In the case of cable television systems, this secure communications path runs directly between the cable headend and the relevant device. Once that secure communications path is established, then any compatible "conditional access" or "digital rights management" software, including those using virtually all current commercially available encryption algorithms, can be employed, or designed to download to the device.[6]

[5] Attached, again, here.

[6] Contrary to the suggestion in footnote 5 of CEA's opposition, the BBT downloadable security solution does indeed meet the "...caveats and explicit expectations" contained in various Commission documents relating to downloadable security.

As noted above, the BBT downloadable security technology is currently in production, the microchip is available from a public vendor (STMicroelectronics), has been incorporated into cable set-top boxes, and is currently being employed in cable systems. The technology is, and has been on public display at the offices of CableLABS in Boulder, Colorado. Significantly, the same technology can be employed in broadband systems, and could be used in existing devices, such as computers, tablets, etc., through the use of technologies such as a totally portable "USB Dongle" containing the secure microchip. The information provider, in that case, would control the encryption, conditional access, etc., from its server once a secure communications path was established. Given that the conditional access parameters can be in the total control of the information provider, and they are downloadable, different providers could and will likely use different forms of security.

While BBT clearly believes that its technology will prove to be the best approach to the challenge of downloadable security, we are not foolish enough to suggest that it is the only approach. Hence, we believe that others should be encouraged to experiment with and deploy their own downloadable security approaches. It is certainly the case, as we have experienced since originally informing the Commission of our technical developments in 2007, that industries move slowly when confronted with new and unique technologies, particularly in the critical area of security. As even the CEA notes, manufacturers are reluctant to move forward before they are assured of customers. Customers are reluctant to move forward until they are assured of multiple options for manufacture. All are hesitant until they can actually see and test new technology in a full, field setting, and very few are willing to be the "test case." BBT has experienced and now overcome all of those hurdles. Charter now wants to "test the waters" of downloadable technology as well.

We believe that innovation should be encouraged in any way possible. We also believe that the

In particular, with the BBT Solution, conditional access functionality is in fact not activated until it is downloaded to the box by the cable operator. Moreover, an unlimited number of conditional access protocols could be downloaded and replaced, seriatim, to the same device. That is one of the fundamental strengths of the BBT approach: it is uniquely flexible and changeable regarding the software security used, thus significantly limiting the current problem of a "trusted authority" embedded code approach to conditional access which experience indicates creates a far too large "threat target" for hackers.

BBT technology will prove to be more secure, more flexible, and less expensive with regard to headend and bandwidth requirements and costs, even for Charter. This is because, so far as we have been able to determine, the BBT design is potentially compatible, at the discretion of the manufacturer, with virtually any current cable security design, including the one proposed by Charter. In addition, as already noted, the willingness of the Commission to allow experimentation has resulted in the BBT design being compatible with all current transmission protocols, including QAM, QPSK, VSB, and IP. In other words, the downloadable security component of the BBT Solution is platform agnostic. That is one of the great strengths that has resulted from the Commission allowing technology to develop instead of freezing it with strict adherence to CableCARD designs that are universally considered obsolete.

CEA has chosen to cite only one example of the multiple efforts by the cable industry to develop downloadable security. That effort, "PolyCipher," failed. But failure, too, is part of any development process. The BBT effort did not fail, and it is entirely possible that Charter's design will also prove effective. As already noted, we would hope that Charter takes a close look at the already-existing BBT design since it may find it far more economically compatible with system configurations requiring many headends serving multiple communities as opposed to the Cablevision configuration mentioned in Charter's petition. The impetus for initially developing the BBT technology, as explained in the aforementioned White Paper, was specifically to respond to a need in these markets as well as be equally effective in two-way, large, urban settings.[7] Charter's proposal to build and deploy an "integrated security" device that also is designed to migrate to a "downloadable security" regime is both sensible and consistent with the public interest. It certainly contains more promise than simply continuing to require distributors to deploy and consumers to pay for unused CableCARD technology.

II. Clarifying Misimpressions

CEA's opposition raises an issue it has trotted out in the past: the requirement that its members

[7] White Paper at 2

seeking to learn more about the design of downloadable security sign non-disclosure agreements ("NDAs").[8] CEA's comments on this issue are either disingenuous or naive. Most if not all of CEA's membership manufactures devices that contain numerous components from other manufacturers, and specific design components are routinely discussed and disclosed only after NDAs are in place. This is particularly the case when dealing with security issues.

If CEA is suggesting that no downloadable security design can be acceptable so long as it is in some way protected from inappropriate disclosure, then CEA is really just urging the FCC to adopt a ban on all future security developments. That cannot be the case. While we cannot speak for the Charter approach and design, we can say that CEA members have long been offered, and some have signed NDA agreements to learn more about the details of the BBT technology. We have met with, and offered industry-standard NDA agreements to CEA itself. They have chosen not to sign them. That CEA refuses to learn more about the details of the security designs being developed is certainly not an argument to stop development! Additionally, BBT's license fees and technical standards for constructing set-top boxes employing the BBT technology have been available for some time, and have been found acceptable by manufacturers. The assumption that "the industry" will adopt fees and license conditions that will "unfairly" impede competition is demonstrably not true.

As for the "capabilities" of competitive devices, that is an issue wholly apart from downloadable security. Cable boxes, satellite boxes, IPTV boxes, game boxes, dedicated DVR's like TiVo, and service-specific boxes like Boxee and Roku all have different capabilities. They could all, in our view, benefit from downloadable security, and they could all use such downloadable security, at least in the form BBT offers it, and potentially in other forms as well, while all having different market capabilities. The Commission, in considering the issue of downloadable security and its relationship with the broader issues of maintaining any continuing requirement for the failed CableCARD experiment or the proposed AllVid industrial policy, should always keep in mind the distinction

[8] CEA Opposition at 4-5.

between the establishment of a *secure communications path* and conditional access in whatever form. No matter what "interface" may ultimately be proposed that applies to all MVPDs, however defined, security, and within security, the concept of a secure communications path, will be an obvious first necessity. Without that no business plans exist that could support the infrastructure.

BBT has developed an inexpensive, efficient and potentially portable way to establish a secure communications path which then can be used to download various (and multiple) types of conditional access security. Charter is now proposing to experiment with a different approach to the same goal. The Commission should, as it has in the case of BBT, follow the clear desire of Congress to avoid actions which could have the effect of freezing or chilling the development of new technologies and services. It should encourage the development and deployment of downloadable security to continue in whatever way it can.

Respectfully submitted,

BEYOND BROADBAND TECHNOLOGY, LLC

/s/William D. Bauer

William D. Bauer, CEO - CTO
Beyond Broadband Technology, LLC
1140 10th St.
Gering, NE 69341

Stephen R. Effros
Effros Communications
PO Box 8
Clifton, VA 20124
steve@bbtsolution.com
202-596-1305

December 10, 2012

Beyond Broadband Technology / The BBT*Solution*™

A "WHITE PAPER" ON A NEW CONCEPT FOR SECURING THE TRANSMISSION OF ELECTRONIC INFORMATION

Beyond Broadband Technology, LLC, (BBT™) has developed The BBTSolution, an open standard downloadable security system which does not require the use of a "trusted authority". The BBTSolution constitutes a unique method of establishing a secure communications path with either one-way or two-way devices as well as mechanisms for establishing authentication, authorization and reception of encrypted transmissions of voice, video or other data.

Explaining a new concept in the field of information security is never easy. That's particularly the case since various users, purveyors, government regulators and even standards-setting bodies use either very similar or very conflicting definitions for similar terms. This "White Paper" is meant to make clear what we are referring to with the terms being used to explain the BBTSolution, and thereby help to underscore the unique flexibility it can bring to multiple forms of information security.

INFORMATION SECURITY

This is a very broad term, and in the context of the BBTSolution, it is meant that way. The BBTSolution establishes a highly secure communications path between a transmitting device and a receiving device. The transmission medium is not restricted. As is explained below, the BBTSolution was first designed for use with cable television broadband systems. However this OSDS (open standard downloadable security system) is not restricted to any particular communications path, and will also work on IP (Internet Protocol) systems or over-the-air, satellite or other transmission paths just as well. Once a secure, authorized and authenticated communications path is established, the system is totally agnostic to the type of data, or information, transmitted over that path. Thus when we talk about "information security," it could be anything from a television program or channel, or first-run movie to health care or banking information, automated data for controlling the power grid, or any other type of information.

Once the secure communications path is established, the level of security, including authentication, usage restrictions, or any other type of security is user-definable. What makes this approach unique is that because it is "downloadable," security conditions can be changed repeatedly, depending on the use. In other words it can be employed by multiple transmitters of information, each utilizing different types and levels of security. A consumer with a BBTSolution enabled computer (either built-in or in a portable USB "dongle") for instance, could securely access multiple video programmers via the Internet, each with it's own encryption and conditional access protocols. A Veteran could have similar access to all his or her medical records at multiple locations with total security provided by a BBTSolution chip in a USB thumb-drive type device, or embedded in medical facility computers.

THE BASICS

The BBTSolution has two parts; a secure microchip in the receiving device, and an "HSM" (Hardware Security Module) at the transmitting site. The HSM can be integrated into the transmitting location of a cable broadband, satellite, broadcast or telephone system, or it could be a part of any computer server used by a provider of information, Google, for instance, on the Internet. HSM's could also be integrated into devices (such as a host computer) used by doctors or hospitals to transmit patient data or any other data transmission application. The cost of the HSM enabled equipment will vary depending on the use. The current design for cable television systems, including the computer, costs less than $10,000, approximately one-tenth the price of the conditional access headend controllers commonly used in that market today. We anticipate that the basic Hardware Security Module enabled for use on computer servers can cost half that, or even less.

The secure microchip can be incorporated into, as examples, a cable television set-top box, a television set, a digital video recorder, a home, office or laptop computer, or even in a portable USB device (much like a "thumb drive" or "dongle") that could be inserted in any current computer USB port. The chips, which are already being manufactured by one of the best-known secure microprocessor manufacturers in the world, ST-Microelectronics, are inexpensive (they are currently priced at $5.00 including the BBT license fee) and are designed to be integrated into multiple consumer devices, much like the well-known "Dolby™" system is included in most consumer audio devices today.

BOTH TWO-WAY AND ONE-WAY DEVICES

One of the many unique aspects of the BBTSolution is that the receiving device, such as a television set, need not be a "two-way" device. The secure communications path, once established, is totally managed by the transmitting and receiving devices themselves, and the receiving device does not have to be in constant return-path communication with the transmitting HSM enabled equipment. Thus, for instance, with one telephone call a cable television consumer could read a series of numbers that appeared on their television screen to the headend and from that point on the cable HSM enabled headend controller and the consumer's BBTSolution device can establish and maintain a secure authenticated channel (SAC) without the need for two-way communication or bandwidth use. Of course the system will also work, automatically, with two-way communications, such as with IP computer communications on the Internet or in two-way broadband cable systems.

THE ORIGINAL CHALLENGE

The BBT*Solution* was originally designed to respond to a need for a new, low-cost cable television set-top box that could meet government mandates for "separable security" for such devices. Until June of 2007, cable television systems traditionally used a set-top box (a tuner, and descrambler) that had "integrated security". That is, the entire process of assuring that the box belonged to the right customer, was in the right location, and had the proper codes to decrypt only that programming meant for that customer was all integrated into the set-top box. Legislation intended to foster a consumer market for set-top boxes resulted in the FCC establishing rules requiring that the security function be separated from the rest of the functions of the set-top box. This, theoretically, would allow anyone to design new and competitive set-top boxes that could be used in any cable system since the security function was not integrated into the box and could be enabled in each location (which had different security, or "conditional access" systems) another way.

The method originally chosen for this separated function was the CableCARD, a modified version of the PCMCIA (Personal Computer Memory Card International Association) card then in use in personal computers. The idea was that any set-top box could be built with a capability to accept the CableCARD, and that cable systems could supply the appropriate card, which controlled the security, or what has generally been called the "conditional access" components of the system. Unfortunately, CableCARDs are both expensive (both the card and the docking device) and no longer constitute an advanced technology. The PCMCIA design is generally now considered obsolete, and most computers

today no longer incorporate PCMCIA slots, having progressed to new designs such as USB (Universal Serial Bus). The BBTSolution is, however, "backward compatible" with CableCARDS.
One of the original objectives of BBT was to design a new "separable security" system. Several efforts to design such a new system were launched by various companies. Unfortunately, the layman's language used to describe these systems, which was subsequently adopted by the FCC, was "downloadable conditional access systems" or DCAS. We say unfortunate, because this language necessarily confuses the various functions being described, and implies that they are all part of a single, integrated process. While that is a traditional approach to security and conditional access, it is not the only way it can be accomplished. Another of the unique attributes of the BBTSolution is that it separates the establishment of a secure communications path from the other functions of authorization, authentication and encryption /decryption of the data. This allows, as is explained below, almost unlimited flexibility in the use of the system.

A SECURE COMMUNICATIONS PATH -- WITHOUT THE NEED FOR A "TRUSTED AUTHORITY"

The traditional approach to establishing a secure communications path is to use a "public/private encryption key" dialog between devices. However this standard approach also requires that the "private key" be in some way secured and archived for referral and use to authorize the communication. Thus, there must be a "trusted authority" holding and controlling all of the private keys. If those keys are somehow discovered, the entire security system, including all the devices with hardware linked to those keys, if any, are compromised. The BBTSolution does not employ public/private keys or require a "trusted authority," thus eliminating the two most significant vulnerabilities of the traditional approach.

With the BBTSolution, the "public/private" keys that enable devices to securely communicate are replaced by a "symmetrical key" approach. Keys are determined internally by the HSM and the secure micro embedded in the receiving device. Each time the HSM and a receiving device establish a secure communications link new random keys are used, thus there is no need for a "trusted authority" and the risk factor of "hacked" or stolen keys is eliminated. No user needs to rely on any other entity for the maintenance of security of the devices used in its communications. This, in turn, significantly reduces the "threat target" for secure communications. Since each user of the BBTSolution establishes their own conditions for authentication and use, what we term "conditional access," the two parts of the security protocol; establishing the secure communications path and then establishing the authentication, access and use conditions, become additive in their security effect, particularly since they are not static.

DOWNLOADABLE CONDITIONAL ACCESS

The basic BBTSolution does not include "conditional access" protocols. The entire idea behind the early development of this approach, as noted above, was to separate the establishment of the secure communications path from the conditions imposed on the use of data after that communications path was created. Thus the BBTSolution has been designed in an "open" format where specifications will be made available so that anyone can design "conditional access" software that can be downloaded to the receiving BBTSolution-enabled device. This conditional access software can be as simple or as robust as the user chooses. For instance, in the case of a cable television system operator, the conditional access system might be automatically triggered by a known subscriber code number, pin number, or location address. In the case of a portable USB "stick", which could be inserted in any modern computer at any location, a program supplier (ESPN or a movie supplier, as examples) could, once the secure communications path is established, download a customized "conditional access" protocol that required a password, a credit card verification, or some other method of authentication. The relationship between the information provider and the customer over the Internet would be direct, and totally controlled by the conditions imposed by the intellectual property owner. In the case of medical records, it has already been suggested that the USB key or an embedded secure micro at the medical facility could be conditioned to be biometrically authorized, for instance only with thumb print verification, as well as a password to assure security and privacy of personal data.

Once the BBTSolution secure communications path is established, the conditional access protocol of the given information provider is downloaded, and authentication has taken place, then the information distributor can additionally impose any other conditions for the access of the material being sent. Of course at minimum, that information is encrypted. The BBTSolution secure micro includes a "virtual machine" or "tool box" that contains over a dozen of the most commonly used encryption algorithms. These algorithms have all withstood the test of time and have proved to be highly secure. But in the BBTSolution approach they are even more so, because they can be used in any order and any combination, again at the discretion of the information provider. Thus a conditional access protocol could be downloaded instructing the BBTSolution secure micro to use, assuming, for instance, if there were 12 algorithms available, any combination of 12 to the 12th power combination of encryption/decryption processes. However one can never assume that something simply can never be "broken," so the system is designed so that the protocol can be changed at will by the provider, as many times as they wish, and as often as they choose. It is generally acknowledged that a "software-only (DRM--"digital rights management") approach to encryption or conditional access is subject to constant challenge. As the saying goes, "..there's a new crop of 18-year-old hackers every year!" The BBTSolution HSM and microchip, along with a downloadable conditional access component, does not suffer from that same risk. It is a highly adaptable, nimble and very flexible approach to secure communications.

Along with establishing security and conditional access, including any form of additional "DRM" chosen by the information provider, the ability to "download" protocols allows for other flexibility as well. For instance information stored in different formats may require that a "reader" be associated with the information being transmitted. This is particularly true in a field such as health care. Reader programs, with limitations on use, both in terms of time and content, could be downloaded and deleted with each session establishing a secure communications path. Data downloaded to a computer hard drive could be stored only in encrypted form, thus totally protected unless a secure communications path was established to authorize decryption.

CONCLUSION

The BBTSolution is unique. It allows for absolutely secure communication and control of intellectual property and privacy of data transmissions on multiple broadband and narrowband formats. It can enable such communication to devices that are either one-way or two-way capable. It does not require a "trusted authority" and allows for maximum flexibility for individualized conditional access and use. It's potential uses for broadband and the Internet , in particular, can fundamentally change the way those platforms are used today.

ADDENDUM ATTACHED

ADDENDUM – I

Recent events have highlighted the validity of the reasoning behind the BBTSolution™ approach to electronic information and communications security. The experimental "hacking" of the latest proposed algorithm for use in 3G cellular telephony and the increased focus on illegal international efforts to access proprietary data from various secure repositories of corporate information has once again demonstrated the weakness in current security thinking. The vulnerability reported regarding RSA's "SecurID," and the publication of the root key for HDCP (High Definition Content Protection) reinforces this point. Software solutions and "secure repositories" or "trusted authorities" are being challenged regularly and there is no indication that this activity will stop.

The BBTSolution™ answer to that challenge is a design where any attack on the system is anticipated, repairable, and totally limited. There is no "trusted authority." The "threat target" in the BBT approach can be reduced, literally, to single communications events. Each initiation of the BBTSolution™ secure communications path utilizes a totally unique and individualized creation of ephemeral keys. Those keys would have to be broken during the immediate initiation of the communications session, since once the individual session is over, those keys are no longer of any relevance. Further, since each session and associated conditional access protocol is totally controlled (as to timing, duration, content, encryption, etc.,) by the communicating parties, they can change any or all parameters at will. A "hacker" would have to, while the communications session was in progress, ascertain all of those variables, including the methodology and algorithm used for deriving the unique session keys. Portions of that methodology and the algorithms used are variable as well, making any single session "hack" of very limited value.

Rather than try to create a "Fort Knox" that "can't be broken into," BBT has taken a totally different approach, creating a security design that is so nimble and flexible that the extreme effort it would take to compromise the secure communications path could only yield a result, if successful at all, for that single, unique communication. In addition, all system administrators create their own set of variables, encryption and additional conditional access protocols, adding to the overall security for the vast majority of uses.

A REPRESENTATIVE EXAMPLE: ELECTRONIC MEDICAL RECORDS

There are several interrelated issues in the effort to shift to electronic medical records. Not only is individual security and privacy required, but the records themselves, as in the case with the Veterans Administration, for example, may be in different locations and they may not all be uniform. The use of the BBTSolution™ downloadable security design can address all of those challenges.

In order to assure privacy and authentication, a BBTSolution™ secure microchip can be embedded in a personal "USB Dongle" (a form-factor like a "thumb drive") which also incorporates a biometric (thumb print) reader. The veteran could then visit any facility with computers having USB inputs and authenticate his or her right to access the particular medical records by establishing a secure communications path with any repository medical computer having the requisite HSM (Hardware Security Module). The encrypted thumb print data is stored directly on the resident secure microchip. The USB device will not establish any secure communication without that initial authentication. Any additional authentication required, such as a password, an account number or whatever the institution requires with its own pre-established set of conditional access rules, which would be downloaded to the receiving computer upon initiation of the secure communications path, would assure that the encrypted records were only being transmitted to the appropriate location and that only that location had the requisite information to decrypt the files. That decryption capability would, in this example, only last as long as the secure communications path was in place.

The process also anticipates the interim "downloading" of specialized software should the sending and receiving medical facility not have the same capabilities for reading or reviewing the records. It, too, would only be useable so long as the secure communication path was intact, or limited in any other way decided upon.

Of course any other set of variables could be applied to the medical data thus downloaded. It could be time limited and then automatically discarded, it could be decrypted or left entirely encrypted and only accessible during secure communications path sessions with the personalized USB key, or it could be authorized for use by the new medical facility as a repository for the data. All of these options and many more can be made available through the use of easily developed and downloaded computer code. The key to the secure communication of the data is the initialization of the secure communications path, and the multiple options afforded the user through downloadable capability once that path is established.

While we have cited a USB thumb-drive type form factor (currently tested and ready for mass production) in this quick exploration of how the BBTSolution™ can be used to address many of the challenges of electronic health care records security and distribution, there are other form factors that could also be employed, such as a "smart card," or the BBT secure microchip being directly incorporated into a computer laptop or other chip design. In addition, it should be noted, again, that because of the flexibility inherent in the downloadable design, the same chip (in whatever form factor) used for securing electronic medical records, for instance, could also be used to view a movie, download a book, or do anything else requiring an authenticated secure communications path to multiple devices such as computers, laptops, television sets, game consoles, etc.

The whole point behind this (patent pending) approach to broadband security is that it can be used for multiple purposes and each one can be secured in a different way with as much or as little additional conditional access as is deemed necessary by the parties establishing the communications path. Each communications session is unique as to use, content, authentication and any other conditions chosen based on the nature and need of the communicating parties. Because of that flexibility and versatility, the BBTSolution™ security protocol enables far more uses in a more secure manner than current designs.

12 10 12
Contact: Steve Effros
Beyond Broadband Technology / BBT
steve@effros.com
703-631-2099